Book	Board of Education Policies
Section	7000 - Student
Title	Acceptable Use Policy For Technology And The Internet
Code	7130
Status	Active

Acceptable Use Policy for Technology and the Internet

This policy is intended to be read together with the School District's Internet Safety Policy as applicable to School District employees and students.

Introduction

The School District furnishes computers and access to the network and Internet in order to support learning and enhance instruction. By providing access to the Internet, the School District intends to promote educational excellence and to prepare students for an increasingly technological world. The School district is committed to preparing lifelong learners who are ethical and responsible digital citizens. Students will be able to use Information Communication Technologies (ICTs) to communicate in a variety of modes, solve problems creatively, retrieve and manage information, think critically, remain flexible and continue to learn. They will be self-directed learners able to adapt and thrive in a rapidly changing world.

However, the School District also recognizes that with this access come uses and the availability of material which are unrelated to education, and which in many instances are inappropriate for places of learning, and inappropriate for young people in particular.

For this reason, computer, network and Internet facilities are to be used only for educationally appropriate purposes. The School District has taken precautions to restrict access to questionable materials, but students and parents need to know that it is impossible to control all materials.

All staff and students are expected to take individual responsibility for their use of School District computer devices and the Internet. Therefore, the School District requires that all staff and students act responsibly by reading and following its policies regarding Technology and the Internet. VPN access is strictly prohibited for all students and staff. The only exception is for staff who have pre-approved VPN access to select LHRIC applications.

Ultimately, we realize that the parents/guardians of minors are responsible for setting and conveying the standards that their students should follow. Likewise, parents and students must understand that access to School District computer, network and Internet facilities is a revocable privilege, and not a right. **Use of the system can and will be monitored by the School District, and there is no expectation of privacy in student use.**

Applicability and General Principles

These policies apply to all students who use School District computers, or who otherwise gain access to the School District network facilities and/or Internet via computer equipment and/or access lines located in the School District or elsewhere. This includes any remote access which staff and students may gain from off-site, but which involves the use of School District sites, servers, intranet facilities, e-mail accounts or software.

All access to and use of the School District computers, network facilities and Internet must be consistent with the educational goals of the School District. Staff and students must make efficient, ethical and legal utilization of network resources. Staff and students must be aware that material created, stored on, or transmitted from or via the system is not guaranteed to be private. In addition to the fact that the Internet is inherently insecure, School District administrators may review any and all individual computers and/or areas of the network at any time to ensure that the system is being used properly. For this reason, staff and students should expect that any work created on the network or an Edgemont Google account may be viewed by a third party.

Both internal and external Network and Internet access will be provided to authorized users by the assignment of un

Usernames and passwords will be furnished subject to the provisions of this Policy, and such updates or modifications as may hereafter be promulgated.

Computer and network users must respect the integrity and security of the School District's systems and network, ar

The School District makes no warranties of any kind, whether express or implied, for the service it is providing.

The following policies are intentionally broad in scope and, therefore, may include references to resources, technolc

Rules of Conduct and Compliance

Staff and/or students who violate this Acceptable Use Policy may have their access privileges suspended or revoked by the Director of Technology or other district administrator. In addition, because the School District's information networks and systems are used as part of the educational program, the School District's Code of Conduct also applies to network activities. This Acceptable Use Policy is an extension of the Code of Conduct, and the disciplinary penalties set out in the Code of Conduct will apply if the student acts in violation of this Acceptable Use Policy.

Except as otherwise indicated below, all policies and prohibitions regarding users of the network also apply to users of individual School District computers.

1. The network may not be used to download, copy, or store any software, shareware, or freeware. This prohibition specifically includes copyrighted still, video and audio media files. Moreover, only the Director of Technology is authorized to consent to the terms of any software license with respect to downloaded programs.

2. Computer and network users may not add (or attempt to add) any hardware, software, shareware, freeware, or other applications to a School District computer or to the network without the prior written consent of the Director of Technology.

3. The School District's computers and network (including the use of such computers or the network to access the Internet) may not be used for any commercial purposes, and users may not buy or sell products or services through the system.

4. The School District's computers and network (including the use of such computers or the network to access the Internet) may not be used for advertising, political campaigning, or political lobbying.

5. The School District's computers and network (including the use of such computers or the network to access the Internet) may not be used for any activity, or to transmit any material, that violates United States, New York State or local laws. This includes, but is not limited to, fraudulent acts, violations of copyright laws, and any threat or act of intimidation or harassment against another person.

6. The School District is a place of tolerance and good manners. Use of the network or any School District computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability is prohibited. Network users may not use vulgar, derogatory, or obscene language. Network users may not post anonymous messages or forge e-mail or other messages.

7. Computer and network users are strongly advised to use caution about revealing any information on the Internet, or storing such information on the School District's computers or the network, which would enable others to exploit them or their identities: this includes last names, home addresses, Social Security numbers, passwords, credit card numbers or financial institution account information, and photographs. Under no circumstances should a user reveal such information about another person without that person's express or prior consent.

8. Computer and network users may not log on to someone else's account, attempt to access another user's files, or permit anyone else to log on to their own accounts. Users may not try to gain unauthorized access ("hacking") to the files or computer systems of any other person or organization. However, students and staff must be aware that any information stored on or communicated through the School District network may be susceptible to "hacking" by a third party, and such information may be reviewed by the School District at any time, with or without prior notice.

9. Computer and network users may not access websites, or social media applications that contain material that is obscene or that promotes illegal acts. Likewise, use of the network to access, process or store pornographic material (whether visual or written), or material which contains dangerous recipes, formulas or instructions, is prohibited.

10. The attention of all computer and network users is specifically directed to the School District's separate Internet Safety Policy, which applies to all users of School District computer and network facilities, and which is incorporated herein by reference. Any attempt to bypass, defeat or circumvent the Internet Safety Policy Technology Prevention Measures, which are designed to prevent access to visual depictions that are obscene, involve child pornography, or are harmful to minors is punishable as a violation of this Acceptable Use Policy. In addition,
evidence of use of any computer or the network to access, store or disseminate child pornography will be referred to law enforcement authorities for investigation and prosecution as may be appropriate.

11. Computer and network users may not engage in "spamming" (sending irrelevant or inappropriate electronic communications individually or en masse) or participate in broadcast electronic communications (such as

chain letters or other mass communications) unless they are supervised by a teacher and have been given explicit approval to do so.

12. Computer and network users who maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data may be subject to criminal prosecution as well as to disciplinary action by the School District. This prohibition includes, but is not limited to, changing or deleting another user's account; changing the password of another user; using an unauthorized account; damaging any files; altering the system; using the system to make money illegally; destroying, modifying, vandalizing, defacing or abusing hardware, software, furniture or any School District property. Users may not develop programs that harass other users or infiltrate a computer or computer system and/or damage the components of a computer or computer system (e.g., creating viruses, malware) is prohibited.

13. Computer and network users may not intentionally disrupt network traffic or crash the network and connected systems; they must not degrade or disrupt equipment or system performance. Use of School District printers and paper must be reasonable and must be for appropriate school business.

14. As is the case with all student work, computer and network users may not plagiarize, which is a serious academic offense. Plagiarism is "taking ideas or writings from another person and offering them as your own." Credit must always be given to the person who created the article or the idea. A student who, by cutting and pasting, or otherwise reproducing someone else's content, leads readers to believe that what they are reading is the student's original work when it is not, is guilty of plagiarism.

15. Computer and network users must comply with the "fair use" provisions of the United States copyright laws. "Fair use" in this context means that the copyrighted materials of others may be used only for scholarly purposes, and that the use must be limited to brief excerpts. The School District's library professionals can assist students with fair use issues.

16. Computer and network users may not take data, equipment, software or supplies for their own personal use. Such taking will be treated as theft.

17. The School District assumes no responsibility for student, faculty or staff websites created and hosted outside of the District network.

Violations and Consequences

Consequences of violations include but are not limited to:

- Suspension or revocation of information network access;
- Suspension or revocation of network privileges;
- Suspension or revocation of computer access;
- Suspension from school;
- Expulsion from school;
- Criminal prosecution.

In addition, the School District may seek monetary compensation for damages in appropriate cases. Repeated or se

This Acceptable Use Policy is subject to change. The School District reserves the right to restrict or terminate in

Disciplinary penalties involving possible suspension or expulsion from school will be determined in accordance with the School District's Code of Conduct. However, suspension or revocation of access privileges will be determined by school and District-wide administrators acting in consultation with the Director of Technology.

Policy Presented at April 28, 2009 and May 12, 2009 Board of Education Meetings
Public Hearing at May 26, 2009 Board of Education Meeting
Revised Policy Adopted at June 9, 2009 Board of Education Meeting
Revised Policy Presented at April 23, 2013 Board of Education Meeting
Public Hearing at May 14, 2013 Board of Education Meeting
Policy Adopted at May 28, 2013 Board of Education Meeting
Revised Policy Presented at July 12, 2022 Board of Education Meeting
Revised Policy Adopted at August 23, 2022 Board of Education Meeting